CLAIMS

What is claimed is:

1. A method for authenticating a first terminal to a second terminal comprising:

requesting a string from the second terminal;

obtaining the requested string from the second terminal;

merging the obtained string with a password to create an identification code;

receiving an authentication if the identification code matches an identification code expected at the second terminal;

sending information from an information server to the first terminal.

2. The method of Claim 1, wherein the string is a pseudo random number sequence.

3. The method of Claim 1, wherein the string is an element of an ordered series.

4. The method of Claim 1, wherein merging the string comprises merging the string with the password using an applet at the first terminal, the applet executing an encryption algorithm with a unique merging key.

5. The method of Claim 1, wherein merging the string comprises performing a block addition of the string and the password.

6. The method of Claim 5, wherein performing a block addition further comprises performing a permutation to the string and to the password and adding the permutated string and the permutated password.

7. The method of Claim 1, wherein obtaining the requested string comprises receiving a web page containing a program for generating requests and the string.

8. The method of Claim 7, wherein the web page is an HTML page and the program is an applet.

9. The method of Claim 1, further comprising closing the applet after sending the encrypted data and thereby invalidating the string.

10. The method of Claim 1, further comprising opening another communications session using a string that is an element of an ordered series and wherein the string of the prior communications session is the preceding element of the same ordered series.

11. A method for authenticating a first terminal to a second terminal comprising:

creating a string and storing it in association with an identification of a first terminal;

sending the string to the first terminal;

receiving an identification code from the first terminal composed by merging the sent string with a sender password;

comparing the identification code to an expected identification code;

if the identification code matches an expected identification code, then authenticating the first terminal.

12. The method of Claim 11, wherein the string is a pseudo random number sequence.

13. The method of Claim 11, wherein the string is an element of an ordered series.

14. The method of Claim 11, wherein merging the string comprises merging the string with the password using an applet at the sender, the applet executing an encryption algorithm with a unique merging key.

15. The method of Claim 11, wherein merging the string comprises performing a block addition of the string and the password.

16. The method of Claim 15, wherein performing a block addition further comprises performing a permutation to the string and to the password and adding the permutated string and the permutated password.

17. The method of Claim 11, wherein obtaining the requested string comprises receiving a web page containing a program for generating requests and the string.

18. The method of Claim 17, wherein the web page is an HTML page and the program is an applet.

19. The method of Claim 11, further comprising closing the applet after sending the encrypted data and thereby invalidating the string.

20. The method of Claim 11, further comprising opening another communications session using a string that is an element of an ordered series and wherein the string of the prior communications session is the preceding element of the same ordered series.

21. An authentication terminal comprising:

a merge string library coupled to a processor to create a merge string and to store it in association with an identification of a second terminal;

an output device to send the merge string to the second terminal;

an input device to receive an identification code from the second terminal, the identification code, being composed by merging the sent string with a second terminal password;

an identification test library coupled to the processor to compare the identification code to an expected identification code and if the identification code matches an expected identification code, to authenticate the second terminal.

22. The terminal of Claim 21, wherein the string is an element of an ordered series.

23. The terminal of Claim 21, further comprising an encryption library coupled to the processor to generate the expected identification code by merging the merge string with the second terminal password using an encryption algorithm with a merging key unique to the second terminal.

24. The terminal of Claim 21, wherein the terminal is a web server, wherein the input device and the output device communicate over the web and wherein the terminal transmits a web page to the second terminal containing a program for merging the user password and the merge string.